NDIA Cyber Resilient & Secure Weapon Systems Summit Highlights

June 2017

Holly Dunlap

Raytheon

NDIA SSE Committee Chair

Holly.Dunlap@Raytheon.com

Event Purpose

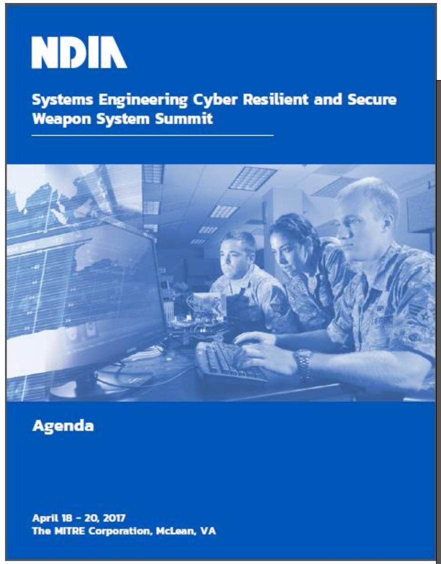
NDIA Systems Engineering Division held a "Top SE Issues Workshop", August 2016

Cyber Resilient & Secure Weapon Systems was identified as a Top SE Issue

System survivability in a cyber contested operational mission environment is critical. We need to elevate the system security risk to the program risk register to ensure a security focus. We need well defined methods, processes, standards, metrics and measures, along with skilled professionals to integrate system security into our product development lifecycle.

***NDIA – National Defense Industrial Association**

Summit Agenda

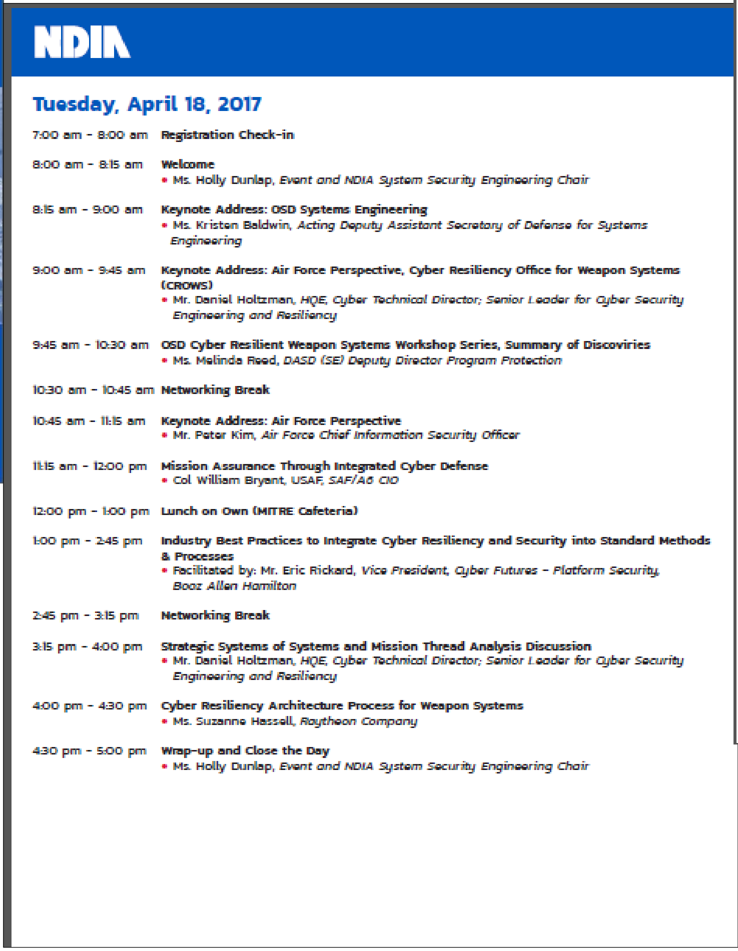


NDIA

Systems Engineering Cyber Resilient and Secure Weapon System Summit

Agenda

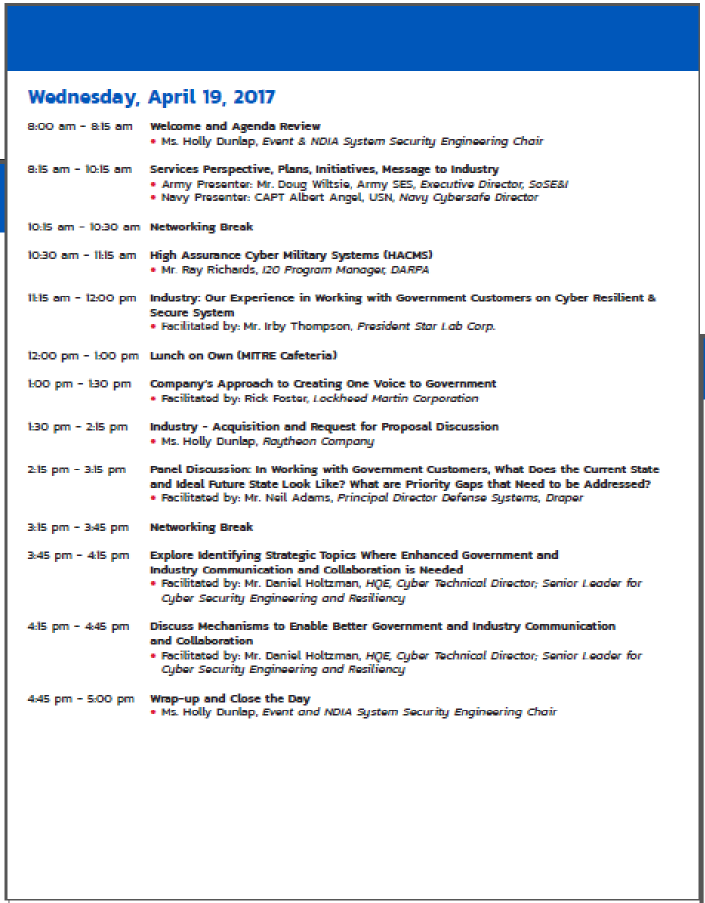
April 18 – 20, 2017
The MITRE Corporation, McLean, VA



NDIA

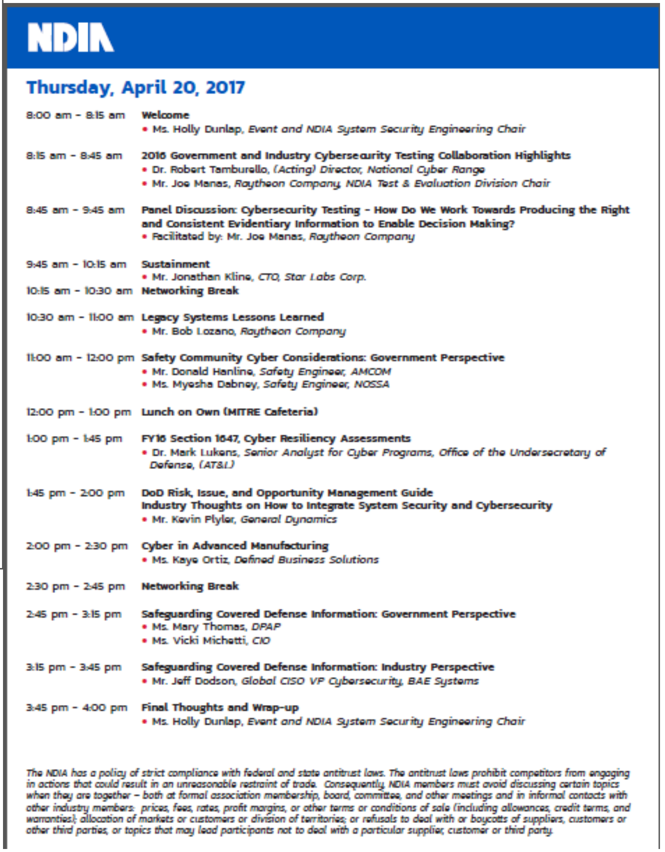
Tuesday, April 18, 2017

7:00 am - 8:00 am	**Registration Check-in**
8:00 am - 8:15 am	**Welcome** • Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*
8:15 am - 9:00 am	**Keynote Address: OSD Systems Engineering** • Ms. Kristen Baldwin, *Acting Deputy Assistant Secretary of Defense for Systems Engineering*
9:00 am - 9:45 am	**Keynote Address: Air Force Perspective, Cyber Resiliency Office for Weapon Systems (CROWS)** • Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*
9:45 am - 10:30 am	**OSD Cyber Resilient Weapon Systems Workshop Series, Summary of Discoviries** • Ms. Melinda Reed, *DASD (SE) Deputy Director Program Protection*
10:30 am - 10:45 am	**Networking Break**
10:45 am - 11:15 am	**Keynote Address: Air Force Perspective** • Mr. Peter Kim, *Air Force Chief Information Security Officer*
11:15 am - 12:00 pm	**Mission Assurance Through Integrated Cyber Defense** • Col William Bryant, USAF, *SAF/A6 CIO*
12:00 pm - 1:00 pm	**Lunch on Own (MITRE Cafeteria)**
1:00 pm - 2:45 pm	**Industry Best Practices to Integrate Cyber Resiliency and Security into Standard Methods & Processes** • Facilitated by: Mr. Eric Rickard, *Vice President, Cyber Futures – Platform Security, Booz Allen Hamilton*
2:45 pm - 3:15 pm	**Networking Break**
3:15 pm - 4:00 pm	**Strategic Systems of Systems and Mission Thread Analysis Discussion** • Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*
4:00 pm - 4:30 pm	**Cyber Resiliency Architecture Process for Weapon Systems** • Ms. Suzanne Hassell, *Raytheon Company*
4:30 pm - 5:00 pm	**Wrap-up and Close the Day** • Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*



Wednesday, April 19, 2017

8:00 am - 8:15 am	**Welcome and Agenda Review** • Ms. Holly Dunlap, *Event & NDIA System Security Engineering Chair*
8:15 am - 10:15 am	**Services Perspective, Plans, Initiatives, Message to Industry** • Army Presenter: Mr. Doug Wiltsie, Army SES, *Executive Director, SoSE&I* • Navy Presenter: CAPT Albert Angel, USN, *Navy Cybersafe Director*
10:15 am - 10:30 am	**Networking Break**
10:30 am - 11:15 am	**High Assurance Cyber Military Systems (HACMS)** • Mr. Ray Richards, *I2O Program Manager, DARPA*
11:15 am - 12:00 pm	**Industry: Our Experience in Working with Government Customers on Cyber Resilient & Secure System** • Facilitated by: Mr. Irby Thompson, *President Star Lab Corp.*
12:00 pm - 1:00 pm	**Lunch on Own (MITRE Cafeteria)**
1:00 pm - 1:30 pm	**Company's Approach to Creating One Voice to Government** • Facilitated by: Rick Foster, *Lockheed Martin Corporation*
1:30 pm - 2:15 pm	**Industry - Acquisition and Request for Proposal Discussion** • Ms. Holly Dunlap, *Raytheon Company*
2:15 pm - 3:15 pm	**Panel Discussion: In Working with Government Customers, What Does the Current State and Ideal Future State Look Like? What are Priority Gaps that Need to be Addressed?** • Facilitated by: Mr. Neil Adams, *Principal Director Defense Systems, Draper*
3:15 pm - 3:45 pm	**Networking Break**
3:45 pm - 4:15 pm	**Explore Identifying Strategic Topics Where Enhanced Government and Industry Communication and Collaboration is Needed** • Facilitated by: Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*
4:15 pm - 4:45 pm	**Discuss Mechanisms to Enable Better Government and Industry Communication and Collaboration** • Facilitated by: Mr. Daniel Holtzman, *HQE, Cyber Technical Director; Senior Leader for Cyber Security Engineering and Resiliency*
4:45 pm - 5:00 pm	**Wrap-up and Close the Day** • Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*



NDIA

Thursday, April 20, 2017

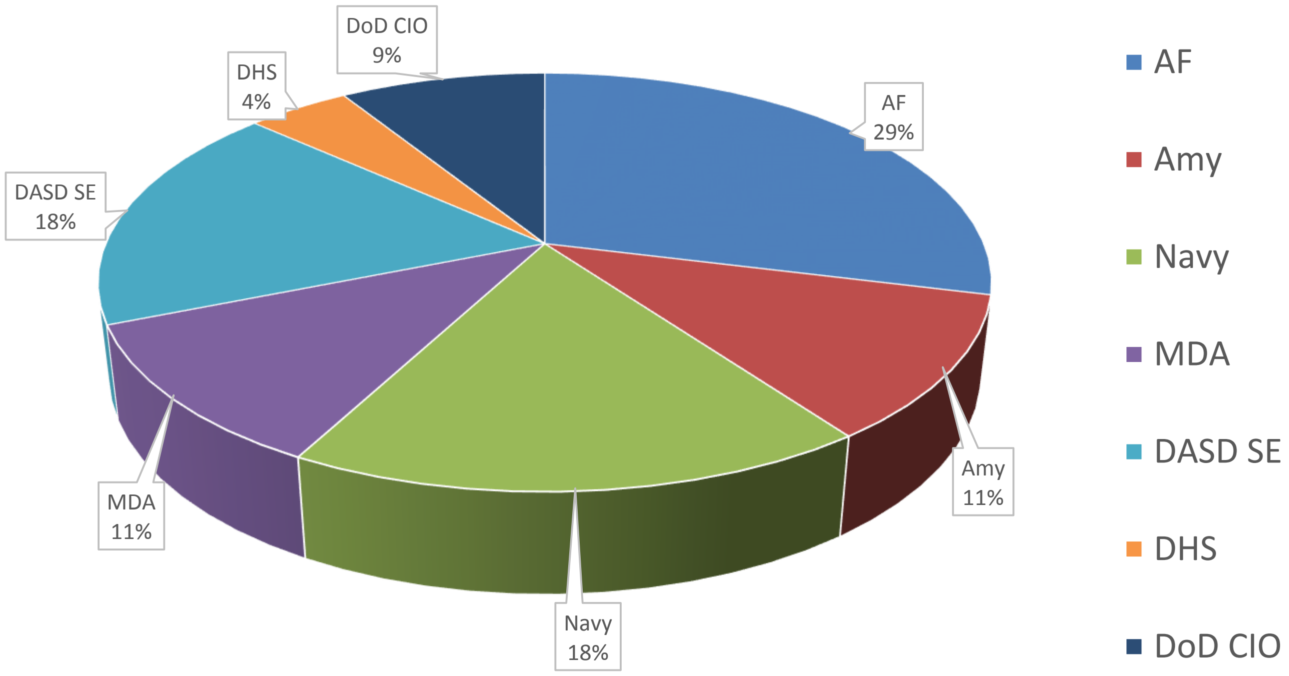
8:00 am - 8:15 am	**Welcome** • Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*
8:15 am - 8:45 am	**2016 Government and Industry Cybersecurity Testing Collaboration Highlights** • Dr. Robert Tamburello, *(Acting) Director, National Cyber Range* • Mr. Joe Manas, *Raytheon Company, NDIA Test & Evaluation Division Chair*
8:45 am - 9:45 am	**Panel Discussion: Cybersecurity Testing – How Do We Work Towards Producing the Right and Consistent Evidentiary Information to Enable Decision Making?** • Facilitated by: Mr. Joe Manas, *Raytheon Company*
9:45 am - 10:15 am	**Sustainment** • Mr. Jonathan Kline, *CTO, Star Labs Corp.*
10:15 am - 10:30 am	**Networking Break**
10:30 am - 11:00 am	**Legacy Systems Lessons Learned** • Mr. Bob Lozano, *Raytheon Company*
11:00 am - 12:00 pm	**Safety Community Cyber Considerations: Government Perspective** • Mr. Donald Hanline, *Safety Engineer, AMCOM* • Ms. Myesha Dabney, *Safety Engineer, NOSSA*
12:00 pm - 1:00 pm	**Lunch on Own (MITRE Cafeteria)**
1:00 pm - 1:45 pm	**FY16 Section 1647, Cyber Resiliency Assessments** • Dr. Mark Lukens, *Senior Analyst for Cyber Programs, Office of the Undersecretary of Defense, (AT&L)*
1:45 pm - 2:00 pm	**DoD Risk, Issue, and Opportunity Management Guide** **Industry Thoughts on How to Integrate System Security and Cybersecurity** • Mr. Kevin Plyler, *General Dynamics*
2:00 pm - 2:30 pm	**Cyber in Advanced Manufacturing** • Ms. Kaye Ortiz, *Defined Business Solutions*
2:30 pm - 2:45 pm	**Networking Break**
2:45 pm - 3:15 pm	**Safeguarding Covered Defense Information: Government Perspective** • Ms. Mary Thomas, *DPAP* • Ms. Vicki Michetti, *CIO*
3:15 pm - 3:45 pm	**Safeguarding Covered Defense Information: Industry Perspective** • Mr. Jeff Dodson, *Global CISO VP Cybersecurity, BAE Systems*
3:45 pm - 4:00 pm	**Final Thoughts and Wrap-up** • Ms. Holly Dunlap, *Event and NDIA System Security Engineering Chair*

The NDIA has a policy of strict compliance with federal and state antitrust laws. The antitrust laws prohibit competitors from engaging in actions that could result in an unreasonable restraint of trade. Consequently, NDIA members must avoid discussing certain topics when they are together – both at formal association membership, board, committee, and other meetings and in informal contacts with other industry members: prices, fees, rates, profit margins, or other terms or conditions of sale (including allowances, credit terms, and warranties); allocation of markets or customers or division of territories; or refusals to deal with or boycotts of suppliers, customers or other third parties, or topics that may lead participants not to deal with a particular supplier, customer or third party.

Who Attended

- **175 Attendees**
  - 33% Government
  - 67% Industry

Government Representation



Industry Representation

- Raytheon
- NGC
- MITRE
- BAE Systems
- Boeing
- Booz Allen
- Draper
- BAH
- Lockheed
- Star lab
- Aerospace Corporation
- General Dynamics
- Rolls Royce
- Textron
- US falcon
- Vencore
- ACET
- ARAR Technology
- BDA/DE
- DBS
- Electronic Warefare associates
- Ensility
- GTRI
- INL
- Innovative Defense Technologies
- Riverside Research
- SAIC
- SEI
- SRI International
- STR
- Synexxus
- Tri Guard Risk Solutions

What We Talked About

Word Cloud

“Cyber Resiliency” in all 27 Topics

27:
Cyber Resiliency

10:
Risk Based Analysis
Mission Thread Analysis
Architecture
Carbon Based Units
Taxonomy

8:
RFP Language
Legacy Systems
Techniques that Work
Culture

7:
Test and Evaluation
Compliance Checklist

6:
SE Responsibility

5:
SSE Role
Domain Expertise
Risk Management Framework
Bake-in
Measurement
Supply Chain
Sustainment

Key Take Away from Services & OSD

- **Affects everyone, responsibility of everyone**
- **SE responsibility to design and deliver systems that are resilient to cyber threat.** Transitioning from Network IT responsibility due to cyber association to SE responsibility to integrate security focus / risk management into the systems we design and deliver.
- **Over 70% of systems in sustainment, how is sustainment addressed**
- **Industry needs to stop promoting magic beans**
- **Acquisition guidance needs to transition to contracts**

- **Biggest challenge is the Carbon Based Units (People)**
- **Risk Management Framework Results**
  - Need to:
    - Improve risk focus instead of compliance & checklist focus
    - Domain expertise is imperative
    - Converge to eliminate duplication and conflicts
    - Test early & often.
  - Not identifying risks correctly, security is coming from IT backgrounds when the security is being applied to mission systems

Challenges from Government to Industry

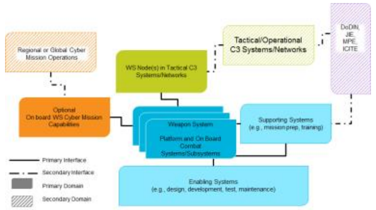
- **Government wants examples from Industry:**
  - Issues to learn from
  - Techniques that work
- **Need help from Industry:**
  - How to improve security with technology that doesn't require redesign
  - How to improve security quickly and efficiently
  - Increase customer confidence in the resiliency & security of the systems we deliver
- **Together we need to address:**
  - What does cyber resiliency look like?
  - How do we measure cyber resiliency?
  - How do we execute and implement cyber resiliency?

Additional key findings:

- Trying to do risk management in an policy/process environment. Need to develop use cases and test cyber system security risk management methods.
- Knowledge of how the system is designed is knowledge of where the risk is, Government does not always have that detail. Government does not fundamentally know how these systems work nor how they are being used. Need help from industry to better understand the system design & capabilities.
- We need to stop taking a reactive approach to our solution. Move away from threat based, b/c it's considered reactive. How do you get the "good" guys to look forward.

Design Patterns, Standards and Methods

What system elements or properties do we acquire?


Regional or Global Cyber Mission Operations
WS Node(s) in Tactical C3 Systems/Networks
Tactical/Operational C3 Systems/Networks
DoDIN, JIE, MPE, ICITE
Optional On board WS Cyber Mission Capabilities
Weapon System
Platform and On Board Combat Systems/Subsystems
Supporting Systems (e.g., mission prep, training)
Enabling Systems (e.g., design, development, test, maintenance)
Primary Interface
Secondary Interface
Primary Domain
Secondary Domain

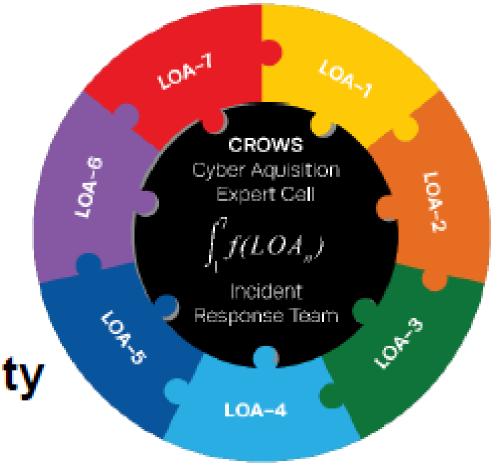
Allocate cybersecurity requirements to the system architecture and design and assess for vulnerabilities. The system architecture and design will address, at a minimum, how the system:

1. Manages access to, and use of the system and system resources;
2. Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment;
3. Is structured to protect and preserve system functions or resources, e.g., through segmentation, separation, isolation, or partitioning;
4. Monitors, detects and responds to security anomalies;
5. Maintains priority system functions under adverse conditions; and
6. Interfaces with DoD Information Network or other external security services.

Draft DTM 118 “Cybersecurity in the Defense Acquisition System” establishes a threshold for what to address

AF CyberCampaign Plan: WeaponSystem Focus

- 7 Lines of Action (LOAs)
  - LOA 1: Perform Cyber Mission Thread Analysis
  - LOA 2: “Bake-In” Cyber Resiliency
  - LOA 3: Recruit, Hire & Train Cyber Workforce
  - LOA 4: Improve Weapon System Agility & Adaptability
  - LOA 5: Develop Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Provide Cyber Intel Support



People, Processes, & Products

- Cyber Squadron Initiatives
- Test & Evaluation (infrastructure & capability growth)
- Industrial Control Systems/SCADA cyber protection measures

Ensure mission success in a cyber contested environment

REDACTED

REDACTED

Industry Themes for Government

- **Policy is mudding the waters**
  - Lots of guidance & standards.
- **Number of Authorities**
  - Unclear of all the relevant & related authorities
  - How many authorities? Who do we listen to and take direction from?
  - Inconsistency in direction
- **Controls and Requirements**
  - Taxonomy
  - Need to be founded and traced to real world scenarios.
- **Challenge Assumptions**
  - Understanding of the CONOPS and how the system is protected throughout the lifecycle.
- **We need to understand the priorities & protection boundaries.**
- **Priorities need to be reflected in RFP and incentivized**

Key Take Aways

- **Focus on mission assurance & not compliance.**
- **Must understand how systems function and the CONOPS**
- **Security must be integrated within Systems Engineering & throughout the system lifecycle**
- **Trace controls ("counter-measure") to specific real-world attack**
- **Cybersecurity testing needs a more structured & integrated approach**
  - Not based on test till the money runs out.
  - How do we produce evidence that provides increased confidence in the system?
- **Need government support to include system security as part of proposals (Section L & M)**

Key Take Aways

- **Need to collaborate to work smarter.**
  - Both Government & Industry want to work together.
- **Everyone is learning. Need to provide customers with risk, cost, performance based trade options.**
- **Mission thread analysis – move from information assurance to mission assurance**
  - Deliver mission assurance through resiliency
  - Assume the attacker is already in the systems.
- **How do we create design standards as enablers and not restrainers?**
- **Post cyber event often results in refining and defining roles & responsibilities and (re)organizational structure. Communication and process are a common theme.**
- **Convergence (integration) before divergence.**
  - Policy, standards, guidance

Specific Actionable Opportunities

- **DoD Risk, Issue, and Opportunity Management Guide**
  - Cybersecurity, Opportunity to shape.
- **Safety Community**
  - JOINT SERVICES-SOFTWARE SAFETY AUTHORITIES
  - Investigate Cyber Considerations - Joint Weapons Software System Safety Process
- **Acquisition / RFP & SOW – Due July 15th**
  - Proposed Section L & M, Review & Comment.
  - AF SSE Guidebook, Review and Comment
- **Systems Engineering Research Center (SERC)**
  - University of Virginia
  - Resilience research efforts, analytically-based decision-support tools
  - Seeking industry partnership to test methods and tools
  - Peter A. Beling
    Associate Professor and Interim Chair
    Department of Systems and Information Engineering
    University of Virginia
    434-982-2066
    beling@virginia.edu